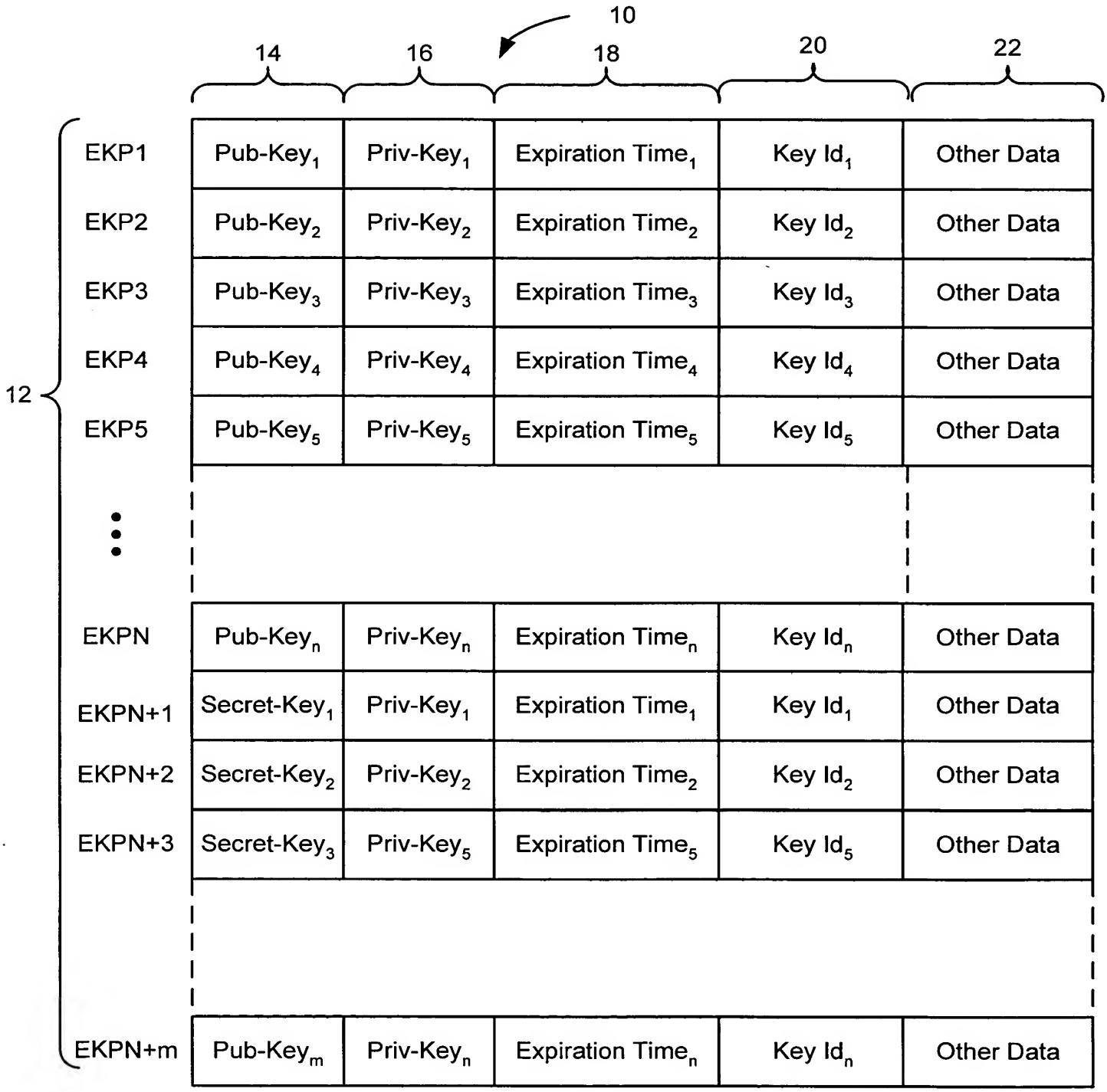
10
14
16
18
20
22
12
EKP1
EKP2
EKP3
EKP4
EKP5
EKPN
EKPN+1
EKPN+2
EKPN+3
EKPN+m
Pub-Key1
Priv-Key1
Expiration Time1
Key Id1
Other Data
Pub-Key2
Priv-Key2
Expiration Time2
Key Id2
Other Data
Pub-Key3
Priv-Key3
Expiration Time3
Key Id3
Other Data
Pub-Key4
Priv-Key4
Expiration Time4
Key Id4
Other Data
Pub-Key5
Priv-Key5
Expiration Time5
Key Id5
Other Data
Pub-Keyn
Priv-Keyn
Expiration Timen
Key Idn
Other Data
Secret-Key1
Priv-Key1
Expiration Time1
Key Id1
Other Data
Secret-Key2
Priv-Key2
Expiration Time2
Key Id2
Other Data
Secret-Key3
Priv-Key5
Expiration Time5
Key Id5
Other Data
Pub-Keym
Priv-Keyn
Expiration Timen
Key Idn
Other Data

Figure 1a

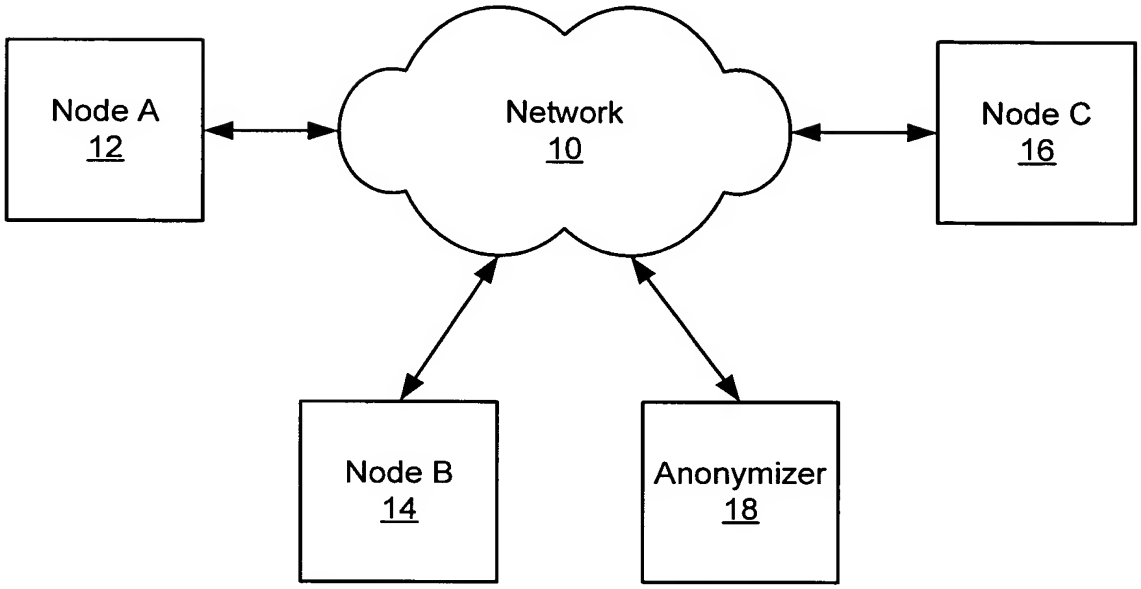
Node A
12
Network
10
Node C
16
Node B
14
Anonymizer
18

Fig. 1b

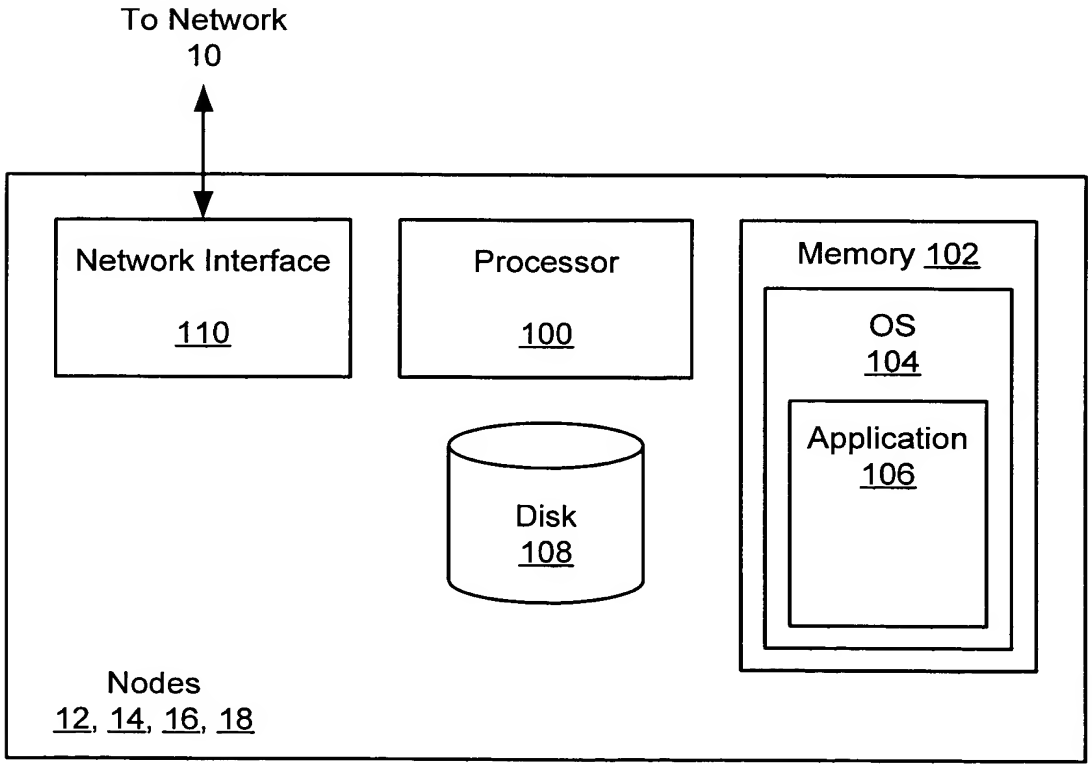
To Network
10
Network Interface
110
Processor
100
Memory 102
OS
104
Application
106
Disk
108
Nodes
12, 14, 16, 18

Fig. 2

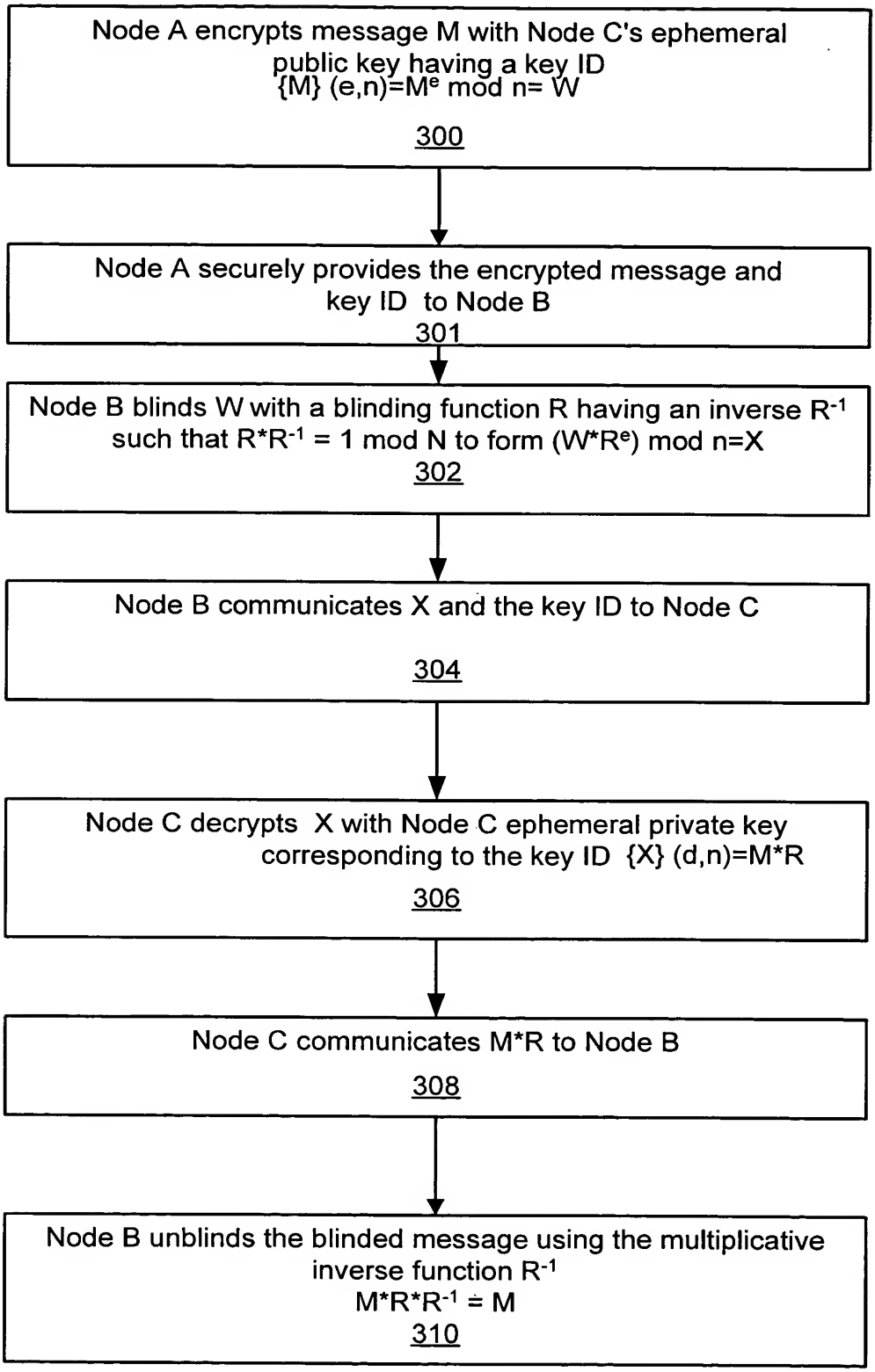
Node A encrypts message M with Node C's ephemeral public key having a key ID
{M} (e,n)=M^e mod n= W
300
Node A securely provides the encrypted message and key ID to Node B
301
Node B blinds W with a blinding function R having an inverse R^-1 such that R*R^-1 = 1 mod N to form (W*R^e) mod n=X
302
Node B communicates X and the key ID to Node C
304
Node C decrypts X with Node C ephemeral private key corresponding to the key ID {X} (d,n)=M*R
306
Node C communicates M*R to Node B
308
Node B unblinds the blinded message using the multiplicative inverse function R^-1
M*R*R^-1 = M
310

Fig. 3

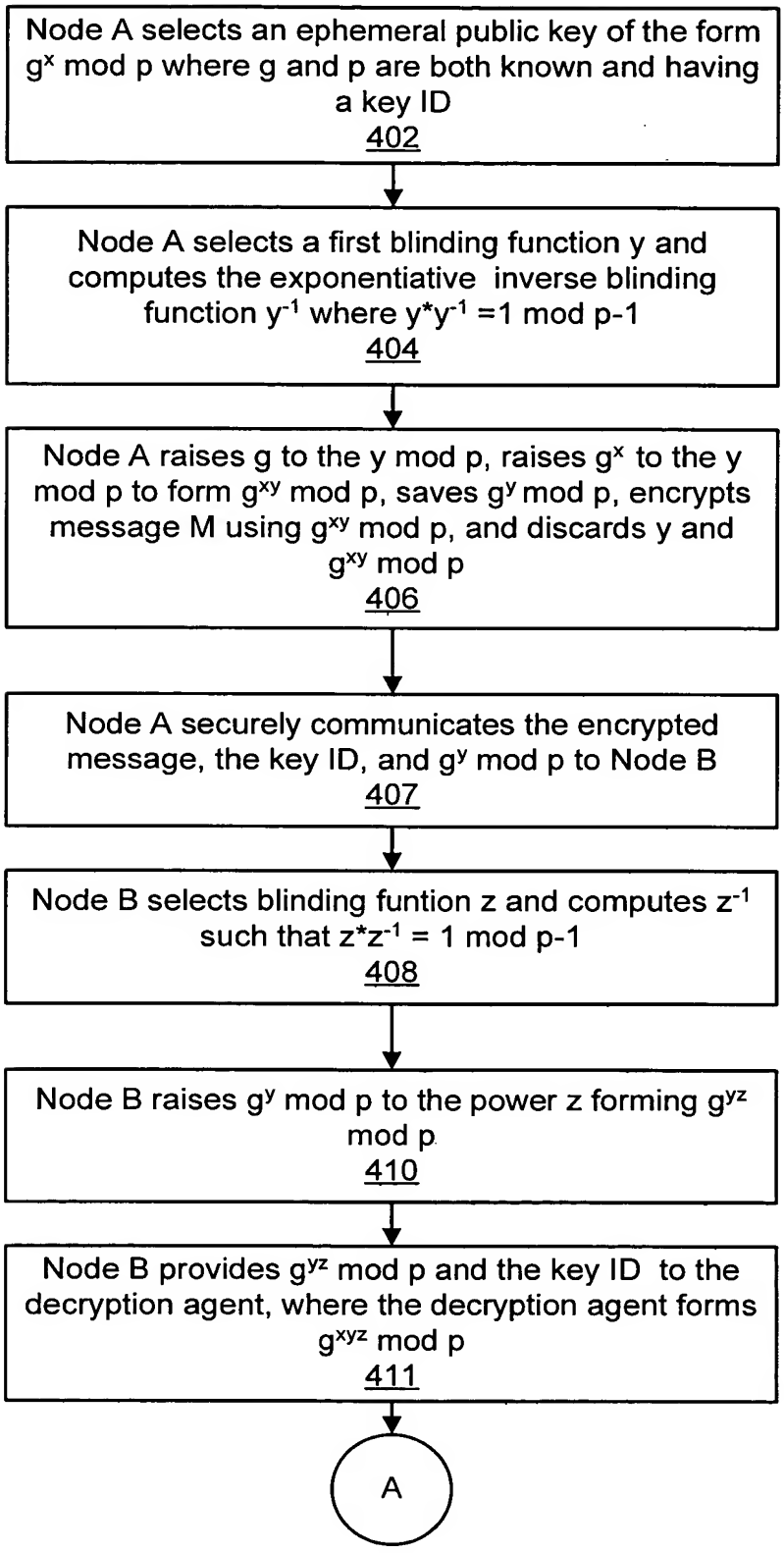
Node A selects an ephemeral public key of the form g^x mod p where g and p are both known and having a key ID
402
Node A selects a first blinding function y and computes the exponentiative inverse blinding function y^{-1} where $y*y^{-1}=1$ mod p-1
404
Node A raises g to the y mod p, raises g^x to the y mod p to form g^{xy} mod p, saves g^y mod p, encrypts message M using g^{xy} mod p, and discards y and g^{xy} mod p
406
Node A securely communicates the encrypted message, the key ID, and g^y mod p to Node B
407
Node B selects blinding funtion z and computes z^{-1} such that $z*z^{-1} = 1$ mod p-1
408
Node B raises g^y mod p to the power z forming g^{yz} mod p
410
Node B provides g^{yz} mod p and the key ID to the decryption agent, where the decryption agent forms g^{xyz} mod p
411
A

Fig. 4a

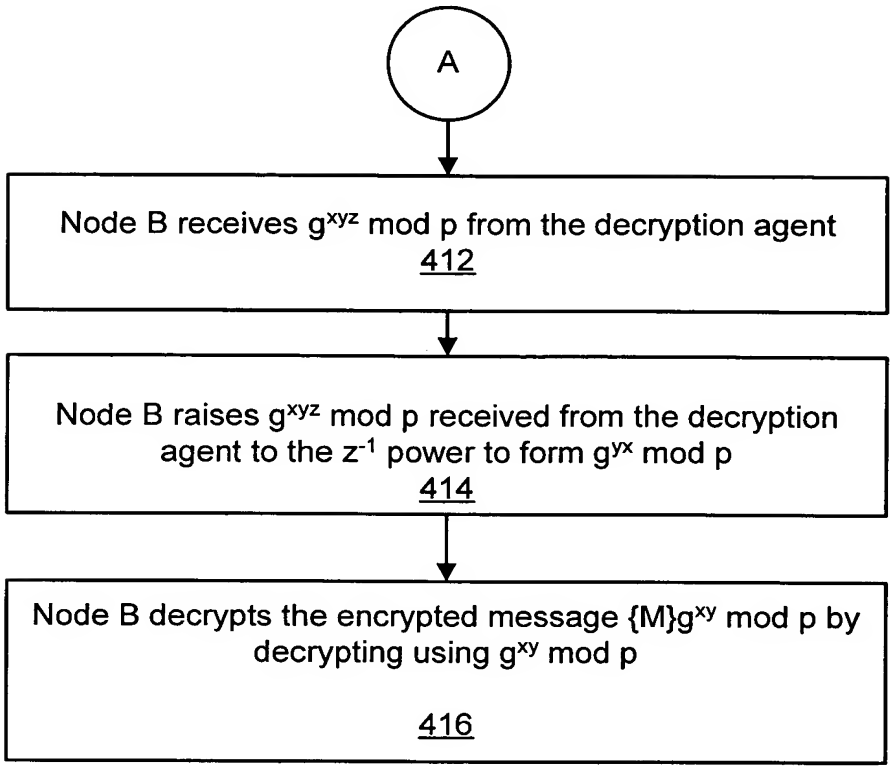
A
Node B receives g^{xyz} mod p from the decryption agent
412
Node B raises g^{xyz} mod p received from the decryption agent to the z^{-1} power to form g^{yx} mod p
414
Node B decrypts the encrypted message $\{M\}g^{xy}$ mod p by decrypting using g^{xy} mod p
416

Fig. 4b

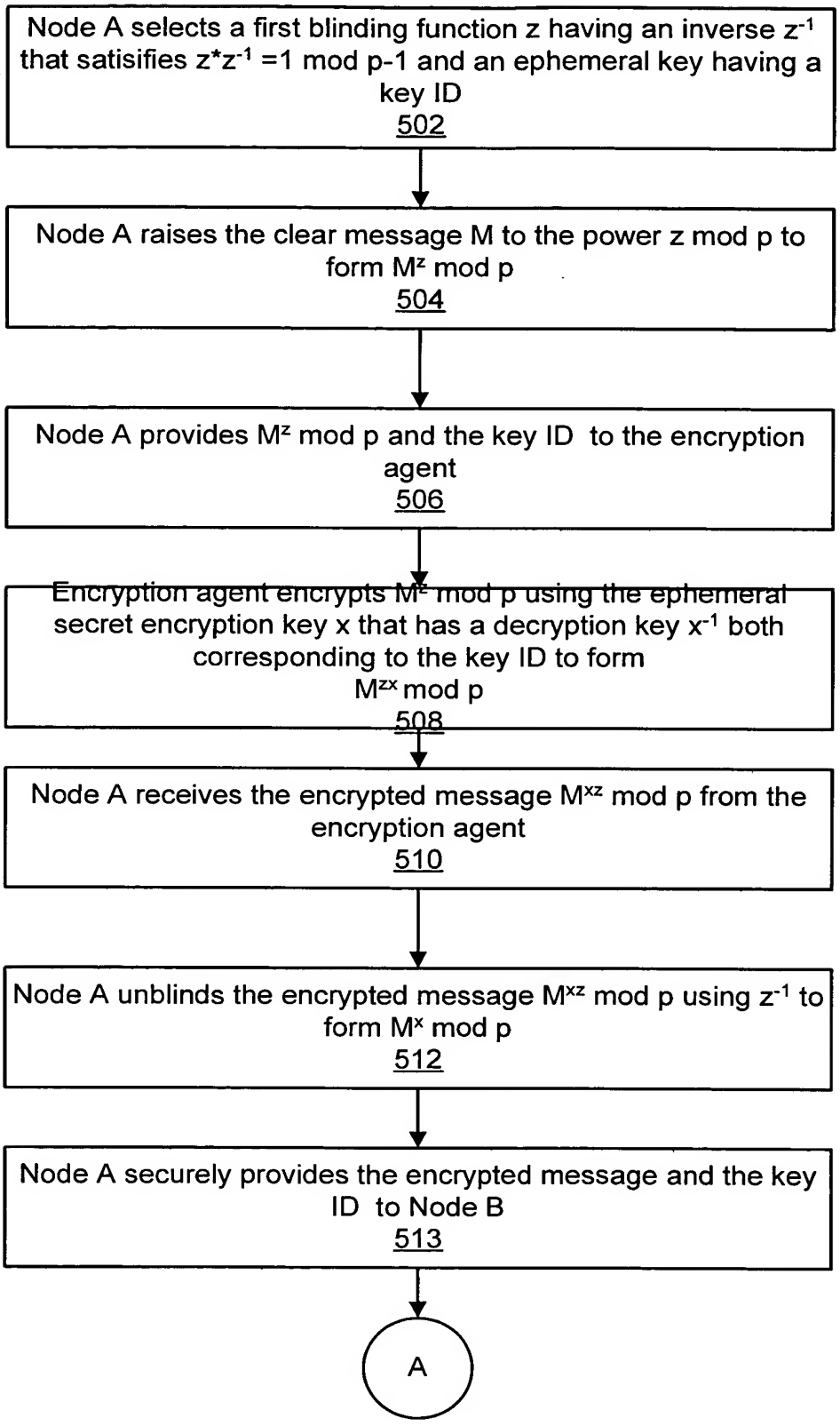
Node A selects a first blinding function z having an inverse z^{-1} that satisifies $z*z^{-1}$ =1 mod p-1 and an ephemeral key having a key ID
502
Node A raises the clear message M to the power z mod p to form M^z mod p
504
Node A provides M^z mod p and the key ID to the encryption agent
506
Encryption agent encrypts M^z mod p using the ephemeral secret encryption key x that has a decryption key x^{-1} both corresponding to the key ID to form M^{zx} mod p
508
Node A receives the encrypted message M^{xz} mod p from the encryption agent
510
Node A unblinds the encrypted message M^{xz} mod p using z^{-1} to form M^x mod p
512
Node A securely provides the encrypted message and the key ID to Node B
513
A

Fig. 5a

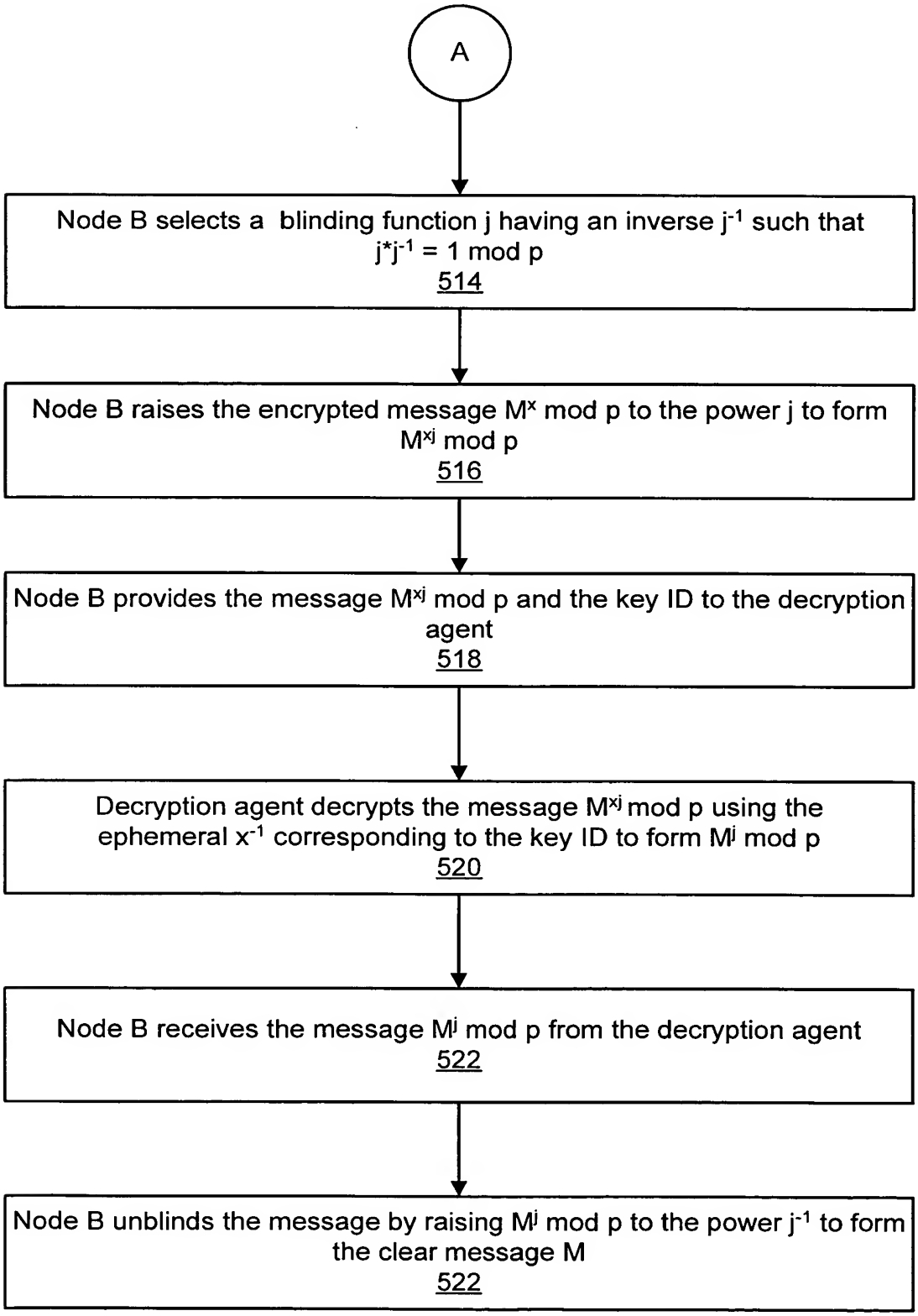
A
Node B selects a blinding function j having an inverse j^{-1} such that $j*j^{-1} = 1 \bmod p$
514
Node B raises the encrypted message $M^x \bmod p$ to the power j to form $M^{xj} \bmod p$
516
Node B provides the message $M^{xj} \bmod p$ and the key ID to the decryption agent
518
Decryption agent decrypts the message $M^{xj} \bmod p$ using the ephemeral x^{-1} corresponding to the key ID to form $M^j \bmod p$
520
Node B receives the message $M^j \bmod p$ from the decryption agent
522
Node B unblinds the message by raising $M^j \bmod p$ to the power j^{-1} to form the clear message M
522

Fig. 5b